

RSD17 Acceptable Use Policy for Student Access to Networked Information Resources

We are pleased to offer the students of Regional School District No. 17 (“District”) access to the school’s computers, networks and the Internet, as well as electronic devices (all of which will be referred to collectively as “computer systems”). Access to the school's computer systems will enable students to explore online resources, including but not limited to libraries, blogs, wikis, databases, websites, and bulletin boards, while exchanging information with others. Such access is provided solely for education-related purposes. Use of the District's computer systems will be allowed only for students who act in a considerate and responsible manner in using such systems.

Regional School District No. 17 believes in the educational value of such electronic services and recognizes their potential to support our curriculum by expanding resources available for staff and student use. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

As the property of Regional School District No. 17 they must be carefully handled and their integrity preserved for the benefit of all. Therefore, Regional School District No. 17 will be treating access to the Internet and the network as a privilege, and not a right, with this privilege controlled by the issuance of an individual password to each student. Students will be required to adhere to a set of policies and procedures, as set forth in detail below. Violations will, at a minimum, lead to withdrawal of the access privilege and cancellation of the password and/or disciplinary measures in accordance with the District’s student discipline policy.

Monitoring

Students are responsible for good behavior on school computer systems just as they are in a classroom or a school hallway. Communications on the computer systems are often public in nature and general school rules for behavior and communications apply. It is expected that users will comply with District standards and will act in a responsible and legal manner, in accordance with District standards, and state and federal laws. It is important that everyone, students and parents, understand that the District, as the owner of the computer systems, both hardware and software, intends to monitor and review the use of this technology to ensure that users engage only in appropriate uses. The District will monitor and review in a limited fashion to maximize utilization of the network for educational purposes.

As part of the monitoring and reviewing process, the District will retain the capacity to bypass any individual password of a student or other user. The system’s security aspects, such as personal passwords and the message delete function for email, can be bypassed for these purposes. The district’s ability to monitor and review is not restricted or neutralized by these devices. The monitoring and reviewing process also includes, but is not limited to, oversight of Internet site access, the right to review emails sent and received, the right to track students’ access to blogs, electronic bulletin boards, instant messages, online communication platforms, and the right to review a student’s data downloading and printing.

Blocking or Filtering Obscene, Pornographic, and Harmful Information

Software blocks or filters material and information that is obscene, pornographic or otherwise harmful to minors from reaching all school computers having Internet or electronic communications access. Students shall report access to material and information that is obscene, pornographic, harmful to minors or otherwise in violation of this policy to the supervising staff member. If a student becomes aware of other students accessing such material or information, the student shall report it to the supervising staff member.

Safety/ Education

The administration will take measures to assure the digital safety and security of students when using electronic messaging systems, email, chat rooms, and other forms of direct electronic communications; to prohibit unauthorized access, including “hacking” and other unlawful activities by minors online; to prohibit unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; to educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response; and to restrict students’ access to online materials that are obscene or obscene as to minors or contain child sexual abuse material, to the extent practicable when students are using Board-owned computers or devices and Board-provided Internet access.

All users must be aware that they should not have any expectations of personal privacy in the use of the network.

Student Conduct

Students are permitted to use the District's computer systems for legitimate educational purposes. Personal use must be specifically authorized by a District staff member. Unauthorized personal use of District computer systems is expressly prohibited. Conduct which constitutes inappropriate use includes, but is not limited to the following:

1. Sending any form of a harassing, threatening, or intimidating message, at any time, to the extent such communication may violate other applicable Board policy, regulation, or school rule (such communications may also be a crime);
2. Gaining or seeking to gain unauthorized access to computer systems;
3. Damaging computers, computer files, computer systems or computer networks;
4. Downloading or modifying computer software of the District in violation of the District's licensure agreement(s) and/or without authorization from a responsible school staff member;
5. Using another person's password under any circumstances;
6. Trespassing in or tampering with any other person's folders, work or files;
7. Sending any message that breaches the District's confidentiality requirements, or the confidentiality of other students;
8. Sending any copyrighted material over the systems;
9. Using computer systems for any personal purpose, or in a manner that interferes with the District's educational programs;
10. Accessing or attempting to access any material that is obscene, obscene as to minors, or contains child sexual abuse material, as defined above;
11. Transmitting or receiving electronic communications or accessing information on the Internet for non-educational purposes;
12. Cyberbullying;
13. Accessing or attempting to access social networking sites (e.g., Facebook, Twitter/X, Instagram, Snapchat, TikTok, YouTube, etc.) without a staff member's authorization and/or a legitimate educational purpose;
14. The unauthorized use of generative artificial intelligence on any of the Board's computer systems. For purposes of this policy, "generative artificial intelligence" refers to a technology system, including but not limited to ChatGPT, capable of learning patterns and relationships from data, enabling it to create content, including but not limited to text, images, audio, or video, when prompted by a user.

In addition, as noted above, if a particular behavior or activity is generally prohibited by law, by Board policy or by school rules or regulations, use of these computer systems for the purpose of carrying out such behavior or activity is also prohibited. Misuse of the computer systems, or violations of these policies and regulations, may result in loss of access to such computer systems as well as other disciplinary action, including suspension and/or expulsion, depending on the specific conduct. Anyone who is aware of problems with, or misuse of, these computer systems, or has a question regarding the proper use of these computer systems, should report or discuss the issue with a teacher or the school principal immediately. Most importantly, the Board and the Administration urge any student who receives any harassing, threatening, intimidating or other improper message through the computer system to report this immediately. It is the Board's policy that no student should be required to tolerate such treatment, regardless of the identity of the sender of the message. Please report these events!

To gain access to the school's networked resources, all students under the age of 18 must obtain parental/guardian permission and must sign and return this form to their classroom/homeroom teacher. Students 18 and over may sign their own forms. No student will be issued a password for access without the receipt of these forms and, to reiterate, access will be limited and controlled by passwords: no password equals no access. Students are responsible for these passwords and should not loan or share their passwords.

Regional School District No. 17 reserves the right to alter, amend, delete or discontinue the foregoing policies in whole or in part at any time and at its absolute discretion.

I have read these guidelines and understand that technology is designed for educational purposes and that access will be supervised in conjunction with curricular objectives.

Student Name

Student Signature

Student ID Number (required)

Parent/Guardian Signature (unless 18 years or older)

Date